CHESTNUT CAMBRONNE PA
Bryan L. Bleichner (CAL BAR # 220340)
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Email: *bbleichner@chesnutcambronne.com*

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

Blake Mijangos, individually and on behalf of all others similarly situated,

Plaintiff,

v.

FI9 Compliance, LLC f/k/a Form I-9 Compliance LLC,

Defendant.

Hon. Judge _____
Case No.: 8:24-cv-2294

CLASS ACTION

COMPLAINT FOR DAMAGES, INJUNCTIVE AND EQUITABLE RELIEF FOR:

1. **NEGLIGENCE;**
2. **INVASION OF PRIVACY;**
3. **UNJUST ENRICHMENT;**
4. **BREACH OF IMPLIED CONTRACT;**
5. **CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL") § 17200 – UNLAWFUL BUSINESS PRACTICE;**
6. **CALIFORNIA UCL § 17200 – UNFAIR BUSINESS PRACTICE;**
7. **BREACH OF CALIFORNIA SECURITY NOTIFICATION LAWS CIVIL CODE § 1798.82**

DEMAND FOR JURY TRIAL

Plaintiff Blake Mijangos ("Plaintiff") brings this Class Action Complaint against FI9 Compliance, LLC f/k/a Form I-9 Compliance, LLC ("Defendant" or "FI9"), in his individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. This class action arises out of the recent targeted cyberattack and data breach in February 2024 ("Data Breach") on Defendant's network that resulted in unauthorized access to its members' sensitive personal data. As a result of the Data Breach, Plaintiff and over 27,000 Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

2. Information compromised in the Data Breach includes individuals' Private Identifiable Information ("PII" or "Private Information") which includes, names, address, Social Security number, date of birth and employment "hire date".

3. Plaintiff brings this class action lawsuit on behalf of himself and those similarly situated to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' Private Information that it collected and maintained.

4. Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

5. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained was exposed and is now in the hands of data thieves.

6. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, obtaining driver's licenses and passports in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

7. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of financial fraud and identity theft.

Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

8. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

9. Through his Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

10. Plaintiff seeks remedies including, but not limited to, compensatory damages, statutory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

11. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserting claims on behalf of the Class (defined *infra*) for negligence, invasion of privacy, unjust enrichment, breach of implied contract, unlawful business practice, unfair business practice, and Breach of California Security Notification Laws Civil Code § 1798.82.

PARTIES

Plaintiff Blake Mijangos

12. Plaintiff received consulting services through Defendant and Plaintiff

received a letter from Defendant dated May 31, 2024, on or about that date (the "Notice of Data Breach Letter"). The Notice of Data Breach Letter notified Plaintiff that "on April 12, 2024, [Defendant] identified unusual activity on its network…[Defendant] has evidence that an unauthorized party accessed or took certain information from [Defendant's] network on February 5, 2024."

13. The Notice of Data Breach Letter informed Plaintiff Blake Mijangos that an unauthorized party accessed Plaintiff's Private Information, including personal information and his Social Security number.

Defendant FI9 Compliance, LLC f/k/a Form I-9 Compliance ("FI9")

14. Defendant is a compliance consulting company in Southern California that acquired, utilized, and stored Plaintiff's and Class Member's Private Information.

15. Upon information and belief, Defendant is headquartered in Newport Beach, Orange County, State of California.

16. Moreover, Defendant's website specifies that it is located in Newport Beach, Orange County, California.

JURISDICTION AND VENUE

17. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs,

there are more than 100 members in the proposed Class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

18. This court has personal jurisdiction over Defendant named in this action because Defendant is headquartered in this District and conducts substantial business in this District.

19. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

ALLEGATIONS

Defendant's Business

20. Defendant is a Limited Liability Company, with its principal place of business in Newport Beach, California.

21. Defendant began operations as a consulting services business in 2004 and is currently serving over 1,000 employers across the United States. [1]

22. FI9 Compliance offers tech solutions and consulting services for Form I-9 and E-Verify compliance, including electronic Form I-9 processing, and automated right-to-work verifications.[2]

[1] *See* https://www.linkedin.com/company/formi9/about/ (last accessed June 4, 2024).

[2] *See* https://www.formi9.com/about-us/ (last accessed June 4, 2024).

23. On information and belief, in the ordinary course of business as a condition of service, Defendant required members, including Plaintiff, to provide copious amounts of sensitive personal and private information, such as the Private Information compromised in the Data Breach.

The Cyberattack & Data Breach

24. On or about April 12, 2024, Defendant identified unusual activity on its network.

25. Defendant immediately began an investigation with the assistance of cybersecurity specialists to determine there is evidence that an unauthorized party accessed or took certain information from Defendant's network on or about February 5, 2024.

26. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members that it would keep their Private Information confidential and protect it from unauthorized access and disclosure.

27. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

Defendant Knew the Private Information on its Network was a Target

28. In light of recent high-profile data breaches at other companies in the consulting industry, Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

29. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[3]

30. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Comply with FTC Guidelines

31. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

[3] *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited June 4, 2024).

32. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

33. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

34. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to

confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

Defendant Failed to Comply with Industry Standards

35. Defendant failed to properly implement basic data security practices.

36. Defendant was at all times fully aware of its obligation to protect the Private Information of its clients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

37. Several best practices have been identified that at a minimum should be implemented by consulting service providers like Defendant, including, but not limited to educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and limiting which employees can access sensitive data.

38. Other best cybersecurity practices that are standard in the consulting industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible

communication system; and training staff regarding critical points.

39. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

40. These foregoing frameworks are existing and applicable industry standards in the consulting industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

DEFENDANT'S BREACH

41. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's negligent failure to protect the confidentiality of Plaintiff and Class Members' Private Information includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect client's Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to adhere to industry standards for cybersecurity.

42. Defendant negligently and unlawfully failed to safeguard Plaintiff and Class Members' Private Information by allowing cyberthieves to access Defendant's computer network and systems which contained unsecured and unencrypted Private Information.

43. Accordingly, as outlined below, Plaintiff and Class Members now face a present and substantially increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at a Present and Substantially Increased Risk of Fraud and Identity Theft

44. Cyberattacks and data breaches at consulting service providers like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

45. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[4]

46. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional

[4] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last accessed June 4, 2024).

confidential or personal information through means such as spam phone calls and text messages or phishing emails.

47. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[5]

48. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

49. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant

[5] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/#/Steps (last accessed June 4, 2024).

being issued in the victim's name.

50. Moreover, theft of Private Information is also gravely serious. Private Information is an extremely valuable property right.[6]

51. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

52. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

53. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

54. Private Information is such a valuable commodity to identity thieves

[6] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

55. There is a strong probability that entire batches of information stolen from Defendant have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at a present and substantially increased risk of fraud and identity theft for many years into the future.

56. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

57. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[7] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

58. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[8] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make

[7] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed June 4, 2024).

[8] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed June 4, 2024).

it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

59. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

60. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[9] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[10] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[11]

---

[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed June 4, 2024).

[10] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed June 4, 2024).

[11] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed June 4, 2024).

61. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[12]

62. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

63. This data, as one would expect, demands a much higher price on the

[12] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed June 4, 2024).

[13] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed June 4, 2024).

black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[14]

64. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

65. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

66. Plaintiff's and Class Members' Private Information was compromised in the Data Breach and is now in the hands of the cybercriminals who accessed Defendant's computer system. Upon information and belief, these cybercriminals have published Plaintiff and Class Members' Private Information to the internet.

67. Plaintiff and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

[14] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed June 4, 2024).

Plaintiff Blake Mijangos's Experiences

68. Plaintiff received consulting services through Defendant.

69. As a condition to receiving the services, Plaintiff provided their Private Information to Defendant, with the expectation that the Private Information would be safeguarded against cyberattacks and foreseeable theft and not disclosed for unauthorized purposes.

70. Plaintiff is very careful about sharing his Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts.

71. Plaintiff only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

72. Plaintiff received the Notice of Data Breach Letter dated May 31, 2024, from Defendant concerning the Data Breach. The Letter stated that the Plaintiff's full name, address, Social Security number, and date of birth were plausibly accessed

or stolen in the Data Breach.

73. Plaintiff suffered injury from a loss of privacy the moment that his Private Information was accessed and exfiltrated by a third party without authorization.

74. Recognizing the substantial risk Plaintiff faces, Defendant provided Plaintiff a two-year subscription to a credit monitoring service.

75. Since learning of the Data Breach, Plaintiff has spent a significant amount of time freezing his accounts, and reviewing bank statements, credit cards, and credit monitoring applications for any fraud or suspicious activity.

76. The Data Breach has caused Plaintiff to suffer significant fear, anxiety, and stress. Plaintiff has lost sleep thinking about all the ways the Sensitive Information that was exposed can be used to commit fraud and identity theft.

77. The risk from the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

78. Plaintiff plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach, such as implementing

credit alerts.

Plaintiff's and Class Members' Injuries and Damages

79. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

80. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

81. Plaintiff and Class Members face the present and substantially increased risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

82. Plaintiff and Class Members face the present and substantially increased risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

83. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

84. Plaintiff and Class Members also suffered a loss of value of their

Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

85. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service or product that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer network and Plaintiff and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for and agreed to.

86. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring Social Security Number, bank accounts, and credit reports for unauthorized activity for years to come.

87. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

88. Further, because of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

CLASS ACTION ALLEGATIONS

89. This action is properly maintainable as a class action. Plaintiff brings this class action on behalf of himself, and all others similarly situated pursuant to Fed. R. Civ. P. 23, for the following Class and Subclass defined as:

> Nationwide Class: All individuals and entities residing in the United States whose Private Information was compromised in the Data Breach that occurred on, or around, February 5, 2024.

California Subclass: All individuals and entities residing or have resided in California whose Private Information was compromised in the Data Breach on, or around, February 5, 2024.

90. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

91. Plaintiff reserves the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

92. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. The Classes are apparently identifiable within Defendant's records as the Notice Letter indicates.

93. Commonality and Predominance: Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. Among the questions of law and fact common to the Classes that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Defendant was unjustly enriched by failing to properly protect Plaintiff and Class Members' Private Information;

m. Whether Plaintiff and Class Members are entitled to restitution as a

result of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

94. Typicality: Plaintiff's claims are typical of those of the other members of the Classes because Plaintiff, like every other member, was exposed to virtually identical conduct and now suffers from the same violations of the law as other members of the Classes

95. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Nationwide Class as a whole and to the California Subclass as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Classes each as a whole, not on facts or law applicable only to Plaintiff.

96. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the

rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

97. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

98. Plaintiff and Class Members are ascertainable because Defendant's records will identify all victims of Defendant's Data Breach.

99. Plaintiff and Class Members are sufficiently numerous as to justify class action. Specifically, upon information and belief, the putative Class exceeds 27,000 individuals.

100. Plaintiff and Class Members have a well-defined community of interest

in pursuing relief from the harm that resulted from the Data Breach, including (1) predominant common questions of law or fact; (2) a class representative with claims or defenses typical of the class; and (3) a class representative who can adequately represent the class.

101. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

102. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

103. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

104. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

105. Plaintiff and the Class repeat and reallege each and every allegation in the Complaint as if fully set forth herein.

106. As a condition of receiving services from Defendant, Defendant's current and former clients were obligated to provide Defendant with their Private Information.

107. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would use reasonable measures to protect their Private Information and only make disclosures to third parties that are authorized.

108. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer

if the Private Information were wrongfully disclosed.

109. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

110. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

111. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' Private Information that Defendant was no longer required to retain pursuant to regulations or legitimate business purposes.

112. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Class.

113. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant on the one hand and Plaintiff and the Class on the other. That special relationship arose because Plaintiff

and the Class entrusted Defendant with their confidential Private Information, a necessary part of receiving services from Defendant. The special relationship also arose as a result of the nature of the relationship between Defendant and its clients.

114. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

115. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

116. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that information, and the necessity for encrypting or redacting Private Information stored on Defendant's systems.

117. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions to not comply with industry standards for the safekeeping of the Private Information of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

118. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

119. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

120. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

121. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiff and the Class.

122. Defendant has admitted that the Private Information of Plaintiff and the Class was accessed, exfiltrated, and published on the internet by cyber criminals.

123. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and the Class during the time the Private Information was within Defendant's possession or control.

124. Defendant improperly and inadequately safeguarded the Private

Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

125. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiff and the Class in the face of increased risk of theft.

126. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former patients' Private Information.

127. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

128. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the present harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and

maintaining appropriate security measures.

129. Defendant's violation of California and federal statutes also constitute negligence *per se*. Specifically, as described herein, Defendant has violated California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to undertake reasonable measures to safeguard the Private Information of Plaintiff and the Class.

130. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the

Private Information of Plaintiff and the Class; and (viii) costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

131. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

132. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

133. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

SECOND CAUSE OF ACTION
INVASION OF PRIVACY
(On behalf of Plaintiff and the Nationwide Class)

134. Plaintiff and the Class repeat and reallege each and every allegation in

the Complaint as if fully set forth herein.

135. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

136. Defendant owed a duty to its current and former clients, including Plaintiff and the Nationwide Class, to keep their PII contained as a part thereof, confidential.

137. Defendant failed to protect and actually or potentially released to unknown and unauthorized third parties the PII of Plaintiff and the Nationwide Class.

138. Defendant allowed unauthorized and unknown third parties to actually or potentially access and examine the PII of Plaintiff and the Nationwide Class, by way of Defendant's failure to protect the PII. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Nationwide Class is highly offensive to a reasonable person.

139. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Nationwide Class disclosed their PII to Defendant as part of Plaintiff's and the Nationwide Class's relationships with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure.

140. Plaintiff and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

141. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff and the Nationwide Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

142. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Nationwide Class.

143. Moreover, as a result of the Data Breach, Plaintiff's Private Information is a private fact as a result of the Data Breach, Defendant publicly disclosed Plaintiff's and Class Members' private facts.

144. Plaintiff and Class Members' Private Information constitutes a private fact.

145. As a result of the Data Breach, Defendant publicly disclosed Plaintiff's and Class Members' Private Facts.

146. Defendant's public disclosure of Plaintiff's and Class Members' Private Facts was offensive and objectionable to the reasonable person and is not of a legitimate public concern.

147. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Nationwide Class was accessed by third parties without authorization, causing Plaintiff and the Nationwide Class to suffer damages.

148. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Nationwide Class in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Nationwide Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Nationwide Class.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class)

149. Plaintiff and the Class repeat and reallege each and every allegation in the Complaint as if fully set forth herein.

150. Defendant benefited from receiving Plaintiff and Class Members' Private Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

151. Defendant also understood and appreciated that Plaintiff's and Class Members' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

152. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of providing their Private Information to Defendant. In connection thereto, Plaintiff and Class Members provided Private Information to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, Plaintiff and Class Members were required to provide their Private Information. In exchange, Plaintiff and Class Members should have received adequate protection and data security for such Private Information held by Defendant.

153. Defendant knew Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

154. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiff and Class Members.

155. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

156. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

157. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

158. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class)

159. Plaintiff and Class Members repeat and reallege each and every allegation in the Complaint as if fully set forth herein.

160. Plaintiff and the Class Members delivered their Private Information to Defendant as part of the process of obtaining services provided by Defendant.

161. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff and Class

Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

162. In providing their Private Information, Plaintiff and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

163. In delivering their Private Information to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

164. Plaintiff and the Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

165. Defendant accepted possession of Plaintiff's and Class Members' personal data for the purpose of providing medical services to Plaintiff and Class Members.

166. Had Defendant disclosed to Plaintiff and Class Members that Defendant did not have adequate computer systems and security practices to secure their Private Information, Plaintiff and Class Members would not have provided their Private Information to Defendant.

167. Defendant recognized that its current and former client's Private Information is highly sensitive and must be protected, and that this protection was

of material importance as part of the bargain to Plaintiff and Class Members.

168. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

169. Defendant breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard their data.

170. Defendant breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their Private Information.

171. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Private Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Private Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff

and the proposed class entrusted Defendant with their Private Information; and (h) the continued and substantial risk to Plaintiff and Class Members' Private Information, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class Members' Private Information.

FIFTH CAUSE OF ACTION
VIOLATION OF CALIFORNIA'S
UNFAIR COMPETITION LAW ("UCL")
UNLAWFUL BUSINESS PRACTICE
(CAL BUS. & PROF. CODE § 17200, *ET SEQ.*)
(On Behalf of Plaintiff and the Nationwide Class or, alternatively, the California Subclass)

172. Plaintiff and the Class repeat and reallege each and every allegation in the Complaint as if fully set forth herein.

173. By reason of the conduct alleged herein, Defendant engaged in unlawful "business practices" within the meaning of the UCL.

174. Defendant stored client data of Plaintiff and the Class Members in its computer systems. Defendant falsely represented to Plaintiff and the Class Members that their Private Information was secure and would remain private.

175. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that would have kept Plaintiff and the Class Member's Private Information secure and prevented the loss or misuse of that Private Information.

176. Even without these misrepresentations, Plaintiff and Class Members

were entitled to assume, and did assume Defendant would take appropriate measures to keep their Private Information safe. Defendant did not disclose at any time that Plaintiff Private Information was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only entity in possession of that material information, which it had a duty to disclose. Defendant violated the UCL by misrepresenting, both by affirmative conduct and by omission, the safety of its computer systems, specifically the security thereof, and its ability to safely store Plaintiff and Class Members' Private Information. Defendant also violated the UCL by failing to implement reasonable and appropriate security measures or follow industry standards for data security, failing to comply with its own posted privacy policies, and by failing to immediately notify Plaintiff and Class Members of the Data Breach. If Defendant had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach, and consequently from, Defendant's failure to timely notify Plaintiff and the Class Members of the Data Breach.

177. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In particular, Plaintiff and Class Members have suffered from improper or fraudulent charges to their credit/debit card accounts; and other similar harm, all as a result of the Data Breach. In addition, their Private Information was taken and is in the hands of those

who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

178. As a result of Defendant's unlawful business practices, violations of the UCL, Plaintiff and the Class Members are entitled to injunctive relief.

SIXTH CAUSE OF ACTION
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL")
UNFAIR BUSINESS PRACTICE (CAL BUS. & PROF. CODE § 17200, *ET SEQ.*)
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the California Subclass)

179. Plaintiff and Class Members repeat and reallege each and every allegation in the Complaint as if fully set forth herein.

180. By reason of the conduct alleged herein, Defendant engaged in unfair "business practices" within the meaning of the UCL.

181. Defendant stored Plaintiff and Class Members' Private Information in its electronic and consumer information databases. Defendant represented to Plaintiff and Class Members that their Private Information was secure, and that Plaintiff and the Class Members' Private Information would remain private. Defendant engaged in unfair acts and business practices by representing that it had

secure computer systems when it did not.

182. Even without these misrepresentations, Plaintiff and the Class Members were entitled to, and did, assume Defendant would take appropriate measures to keep their Private Information safe. Defendant did not disclose at any time that Plaintiff and Class Members' Private Information was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only entity in possession of that material information, which it had a duty to disclose.

183. Defendant knew or should have known it did not employ reasonable measures that would have kept Plaintiff and the Class Members' Private Information secure and prevented the loss or misuse of Plaintiff and the Class Members' Private Information.

184. Defendant violated the UCL by misrepresenting, both by affirmative conduct and by omission, the security of its systems and services, and its ability to safely store Plaintiff and the Class Members' Private Information. Defendant also violated the UCL by failing to implement and maintain reasonable security procedures and practices appropriate to protect Private Information, and by failing to immediately notify Plaintiff and the Class Members of the Data Breach.

185. Defendant also violated its commitment to maintain the confidentiality and security of Plaintiff's and the Class Members' Private Information and failed to

comply with its own policies and applicable laws, regulations, and industry standards relating to data security.

186. **Defendant engaged in unfair business practices under the "balancing test."** The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and misrepresentations to Plaintiff and Class Members about Defendant's data security cannot be said to have had any utility at all. All these actions and omissions were clearly injurious to Plaintiff and the Class Members, directly causing the harms alleged below.

187. **Defendant engaged in unfair business practices under the "tethering test."** Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that ... all individuals have a right of privacy in information pertaining to them.... The increasing use of computers ... has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.") Defendant's acts and omissions, and the

injuries caused by them, are thus "comparable to or the same as a violation of the law …" *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal. 4th 163, 187.

188. **Defendant engaged in unfair business practices under the "FTC test."** The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects tens of thousands of Class Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiff's and the Class Members' Private Information to third parties without their consent, diminution in value of their Customer Data, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiffs' and the Class Members' Private Information remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant's actions and omissions violated, *inter alia*, Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 613 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act); *In re BJ's Wholesale Club, Inc.*,

FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (same); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil Action No. 1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) ("failure to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security. confidentiality, and integrity of personal information collected from or about consumers" violates § 5(a) of FTC Act); 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or[are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

189. Plaintiff and the Class Members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. In particular, Plaintiff and the Class Members have suffered from improper or fraudulent charges to their credit/debit card accounts; and other similar harm, all as a result of the Data Breach. In addition, their Private Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and the Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity

theft losses or protective measures.

190. As a result of Defendant's unfair business practices, violations of the UCL, Plaintiff and the Class Members are entitled to injunctive relief.

SEVENTH CAUSE OF ACTION
BREACH OF CALIFORNIA SECURITY NOTIFICATION LAWS
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the California Subclass)

191. Plaintiff and Class Members repeat and reallege each and every allegation in the Complaint as if fully set forth herein.

192. Pursuant to Civil Code § 1798.82(a), "A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. The disclosure shall be made in the most expedient time possible

and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." Prior to passage of such statute, the California State Assembly cited an incident where authorities knew of the breach in security for 21 days "before state workers were told" as an example of "late notice."

193. Civil Code § 1798.82 further provides, "(h) For purposes of this section, 'personal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number or California Identification Cardnumber. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (4) Medical information. (5) Health insurance information. (i) .... (2) For purposes of this section.

194. Defendant conducts business in California and owns or licenses computerized data which includes the personal information, within the meaning of Civil Code § 1798.82(h), of Plaintiff and the Class.

195. Based upon Defendant's Notice of Data Incident Letter, Defendant was aware that Plaintiff and the Class Members' unencrypted personal information was,

or is reasonably believed to have been, acquired by an unauthorized person no later than April 12, 2024, but did not begin to mail notification letters to Plaintiff and the Class until May 31, 2024. Thus, Defendant waited at least 49 days before *beginning* to inform Plaintiff and the Class of this incident and the subsequent threat to Plaintiff and the Class Members' unencrypted personal information. As a result, Defendant did not disclose to Plaintiff and the Class Members that their unencrypted personal information was, or was reasonably believed to have been, acquired by an unauthorized person, in the most expedient time possible and without reasonable delay in violation of Civil Code § 1798.82(a). Given the example of the Legislature finding that a delay of 21 days to be "late notice" under the statute, Defendant's delay of 49 days before *beginning* to inform Plaintiff and Class Members that their personal information was, or was reasonably believed to have been, acquired by an unauthorized person by mailing Defendant's Notice of Data Security Incident Letter to Plaintiff and Class Members is a presumptively unreasonable notice in violation of Civil Code § 1798.82(a).

196. Upon information and belief, Plaintiff believes and alleges that no law enforcement agency has notified Defendants that the notification would impede a criminal investigation justifying Defendant's decision to wait 49 days *before beginning to mail* notification letters to Plaintiff and Class Members *after* they knew that Plaintiff and Class Members unencrypted personal information on Defendant's

network server was, or was reasonably believed to have been, acquired by an unauthorized person. Upon information and belief, Plaintiff believes and alleges that there were no measures taken by Defendant to determine the scope of the breach or to restore the reasonable integrity of the data system, which justifies Defendant's decision to wait 49 days *before beginning to mail* notification letters to Plaintiff and Class Members. Moreover, FI9's Notice of Data Security Incident Letter mailed to Plaintiff and Class *failed* to state whether notification was delayed as a result of a law enforcement investigation, in violation of Civil Code § 1798.82(d)(2)(D).

197. Plaintiff and Class Members have been injured by fact that Defendants did not disclose to them that their unencrypted personal information was, or was reasonably believed to have been, acquired by an unauthorized person in the most expedient time possible and without reasonable delay in violation of Civil Code § 1798.82(a). Defendant's delays in informing required by Civil Code § 1798.82(a) and providing all of the information required by Civil Code § 1798.82(d) to Plaintiff and Class Members that their unencrypted personal information was, or was reasonably believed to have been, acquired by an unauthorized person, have prevented Plaintiff and Class Members from taking steps in the most expedient time possible to protect their unencrypted personal information from unauthorized use and/or identify theft.

198. As a direct and proximate result of Defendant's and/or its employees'

above-described conduct in violation of Civil Code § 1798.82(a), Plaintiff and Class Members seek damages suffered, according to proof, pursuant to Civil Code § 1798.84(b), and injunctive relief pursuant to Civil Code § 1798.84(e), from the Defendant.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and their Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the

privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment and/or post-judgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

DATED: October 22, 2024

Respectfully Submitted,

/s/ *Bryan L. Bleichner*

CHESTNUT CAMBRONNE PA
Bryan L. Bleichner (CAL BAR # 220340)
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Email: *bbleichner@chesnutcambronne.com*